European Scientific Journal June 2014 /SPECIAL/ edition vol.2 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431

A PROPOSED SECURITY ARCHITECTURE FOR ESTABLISHING PRIVACY DOMAINS IN E-HEALTH CLOUD

Al-Khanjari, Z.
Al-Ani, A.
Al-Hermizy, S.
Department of Computer Science, College of Science, Sultan Qaboos University, Oman

Abstract

Information and communication technology (ICT) are becoming a natural part in healthcare. Instead of keeping patient information inside a written file, you can find all information stored in an organized database as well defined files using a specific system in almost every hospital. But those files sometimes got lost or information was split up in files in different hospitals or different departments so no one could see the whole picture from this point we come up with our idea. One of this paper targets is to keep that information available on the cloud so doctors and nurses can have an access to patient record everywhere, so patient history will be clear which helps doctors in giving the right decision. We present security architecture for establishing privacy domains in e-Health bases. In this case, we will improve the availability of medical data and provide the ability for patients to moderate their medical data. Moreover, e-Health system in cloud computing has more than one component to be attacked. The other target of this paper is to distinguish between different kinds of attackers and we point out several shortcomings of current e-Health solutions and standards, particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-Health systems. To fill this gap, we present security architecture for establishing privacy domains in e-Health infrastructures. Our solution provides client platform security and appropriately combines this with network security concepts.

Keywords: ICT, Healthcare, e-Health, database, cloud computing, security, curious person

Introduction

In the past, information about patients, the illnesses they have had, when they had operations and what medicines they took was written down and kept in files inside hospitals where they have been treated. The problem was that files got lost in different hospitals and doctors cannot get a clear picture about patient's history.

Information systems are now being updated to help to improve healthcare services for all patients. This is to make sure that doctors, nurses and other health professionals have the information that is important to help them to make the best decisions about the patient, their illness and their treatment [7]. Hans and colleagues [1] explored the point out several shortcomings of current e-Health solutions and standards; particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-Health systems. The solution provides client platform security and appropriately combines this with network security concepts. Moreover, Hans and colleagues further discuss open problems and research challenges on security, privacy and usability of e-Health Cloud systems. Henry and colleagues [2] described the presentation of a patient assessment tool compliant with European standards (CEN EN13606, TS14796), and using terminologies describing patient outcomes (C-HOBIC) and nursing practices (ICNP). The demonstration includes the capture of data from assessment forms, and the generation of data views specific to the interests of health service providers and the patient. Barua and Liang [3] proposed an Efficient and a Secure Patient-centric Access

Control (ESPAC) scheme which allows data requesters to have different access privileges based on their roles, and then assigns different attribute sets to them. Extensive security and performance analyses demonstrate that the ESPAC scheme is able to achieve desired security requirements with acceptable communication delay. Gunter and Terry [4] designed a system to represent data that accurately captures the state of the patient at all times. It allows for an entire patient history to be viewed without the need to track down the patient's previous medical record volume and assists in ensuring data is accurate, appropriate and legal. It reduces the chances of data replication as there is only one modifiable file, which means that the file is constantly up to date when viewed at a later date and eliminates the issue of lost forms or paperwork. Due to all the information being in a single file, it makes it much more effective when extracting medical data for the examination of possible trends and long term changes in the patient. Marcio and colleagues [9] presented ClinMalDB, a database system that integrates clinical histories of malaria patients, samples obtained from them, and sequence information of coding genes and includes the technical description of the database, the parameters used to evaluate clinical data of patients, a pre-annotation sequence analysis pipeline service of virulent subtelomeric genes, cube views of the current database, a web-based structure for access and update and an interactive page to illustrate sequence search based on clinical data. The proposed architecture is based on the project of modularization, which divide the whole database into four system levels.

Zhang and colleagues [10] identified a set of security requirements for e-Health application Clouds and proposed a novel security model. This model is mainly designed for the sharing of Electronic Health Records (EHR), while the DACAR platform aims to support the development, integration and large scale deployment of a wider range of e-Health services. Kilic and colleagues [11] proposed to share EHRs among multiple e-Health communities over a peer-to-peer network. A super-peer is used to represent an e-Health community, which is responsible for routing messages and adapting different meta data vocabularies used by different communities. This super-peer design is similar to a Single Point of Contact (SPoC) of the DACAR platform, yet a SPoC provides more authentication and authorisation functionalities. For a patient-centric e-Health platform it is crucial to obtain various patients' consents in an electronic way.

This paper proposes a security architecture for establishing privacy domains in e-Health infrastructures. The paper will discuss security aspects that need to be taken into consideration in the context of e-Health system in cloud computing and provide a rigorous security analysis. Moreover, the paper discusses new methods that can be applied to e-Health systems to counteract the identified threats and thus to establish a very high level of security. The proposal of personal health system is a digital collection of all pertinent medical data of a person that is under control of the subject of care an individual. These data is either entered by the individual or contributed by other information systems. The system proposal could be used to improve the availability of medical data and to provide a comfortable possibility for patients to moderate their medical data. Moderation comprises not only the management of medical data but also the task of granting access to medical data to other parties.

The rest of the paper is organized as follows: Section 2 explains the model of the e-Health Cloud and its relation to medicine, healthcare and information technology and what types of the cloud Service Models and the deployment model for a cloud computing and what the characteristics of e-Health. Section 3 discusses about the Electronic Health Record (EHR) and the difference between the terms EHR, EPR (Electronic Patient Record) and EMR (Electronic Medical Record) and the Benefits of EHR in cloud computing and what the barriers and challenges of e-Health Cloud and the stages of e-Health Cloud. Section 4 describes the purpose of the development of e-Health system in cloud computing and also explains the different types of attacks in cloud computing and the Enhanced Security

Properties of e-Health Cloud and the privacy domains for e-Health. Section 5 provides concluding remarks of the work.

Model of the e-Health Cloud

Everyone is talking about cloud computing today, but not everyone mean the same thing when they do. While there is this general idea behind the cloud – that applications or other business functions exist somewhere away from the business itself – there are many iterations that companies are looking for in order to actually use the technology. Cloud computing offers a variety of ways for businesses to increase their IT capacity or functionality without having to add infrastructure, personnel, and software in their business. Also, cloud computing is available 24/7, which allows people to work when they want to, not restricting them to office hours only [15].

Service Models

According to the different types of services offered, cloud computing can be considered to consist of three layers [12]:

- Cloud Software-as-a-Service (SaaS): This provides the use of applications running on the cloud provider's infrastructure. These services can be accessed from any heterogeneous system or any interface. These services may be defined with exception of limited user specific usage.
- Product-as-a-Service (PaaS): This provides development platform for the user to develop applications using the tools provided by the PaaS provider.
- Cloud Infrastructure-as-a-Service (IaaS): This provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources. This way enables the consumer to deploy and run arbitrary software, which can include operating systems and applications [13, 14].

Deployment Models

Each company chooses a deployment model for a cloud computing solution based on their specific business, operational, and technical requirements. There are four primary cloud deployment models listed as follows:

- Public Cloud: This is the deployment model that is most commonly described as cloud computing. In this model, all of the physical resources are owned and operated by a third party cloud computing provider.
- Private Cloud: This model describes computer services that are delivered to a single organization.
- Community Cloud: This model contains features of both the public and the private cloud models.
- Hybrid Cloud: This model employs aspects of all other cloud models and it is the most commonly found cloud deployment model used within large organizations [16].

E-Health Characteristics

E-Health Cloud computing exhibits the following key characteristics [17]:

- Improves users' ability to re-provision technological infrastructure resources.
- Offers Application Programming Interface (API) accessibility to software that enables machines to interact with cloud software in the same way as the user interface facilitates interaction between humans and computers.
- Claims the reduction of the computing cost, since in a public cloud delivery model capital expenditure is converted to operational expenditure.

- Provides device and location independence. This enables users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone).
- Uses virtualization technology that allows servers and storage devices to be shared and utilization to be increased. Applications can easily be migrated from one physical server to another.

E-Health Services

This term parenthesizes range of services or a system that has relation to medicine, healthcare and information technology, including [5]:

Electronic Health Records: enable the communication of patient data between different healthcare professionals (GPs, specialists etc.);

- E-Prescribing: enable access to prescribing options, printing prescriptions to patients and sometimes electronic transmission of prescriptions from doctors to pharmacists;

Telemedicine: provide physical and psychological treatments at a distance, including telemonitoring of patient's functions;

Consumer health Informatics: use of electronic resources on medical topics by healthy individuals or patients;

Health knowledge Management: access to knowledge, information, experience and best practice in health and social care, overview of latest medical journals, best practice guidelines or epidemiological tracking;

Virtual Healthcare Teams: consist of healthcare professionals who collaborate and share information on patients through digital equipment;

M-Health: include the use of mobile devices in collecting aggregate and patient level health data, providing healthcare information to practitioners, researchers, and patients, real-time monitoring of patient vitals, and direct provision of care (via mobile telemedicine);

Medical Research Using Grids: provide powerful computing and data management capabilities to handle large amounts of heterogeneous data;

Healthcare Information Systems: offer software solutions for appointment scheduling, patient data management, work schedule management and other administrative tasks surrounding health.

Electronic Health Record (EHR)

An electronic health record (EHR) is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. Digitized health information systems are expected to improve efficiency and quality of care and, ultimately, reduce costs. The EHR typically includes:

- Contact information.
- Information about visits to health care professionals.
- Allergies.
- Insurance information.
- Family history.
- Immunization status.
- Information about any conditions or diseases.
- A list of medications.
- Records of hospitalization.
- Information about any surgeries or procedures performed.

Benefits of EHR

- The ability to automatically share and update information among different offices and organizations.
- More efficient storage and retrieval.
- The ability to share multimedia information, such as medical imaging results, among locations.
- The ability to link records to sources of relevant and current research.
- Easier standardization of services and patient care.
- Provision of decision support systems (DSS) for healthcare professionals.
- Less redundancy of effort.
- Lower cost to the medical system once implementation is complete.

Although differences between the terms EHR, EPR and EMR can be defined, they are often used interchangeably. The EMR can, for example, be defined as the patient record created in hospitals and ambulatory environments. It can serve as a data source for the EHR. It is important to note that an EHR is generated and maintained within an institution. These institutions could be a hospital, integrated delivery network, clinic, or physician office. They are used to give patients, physicians and other health care providers, employers, and payers the ability to access patient's medical records across facilities. In modern parlance, a personal health record (PHR) is generally defined as an EHR that the individual patient controls [6]. Health data are very sensitive and need to be protected against misuse by unauthorized persons. Additionally, services which provide online access to health data are even more attractive to attackers. An electronic health record (EHR) is an evolving concept defined as a systematic collection of electronic health information about individual patients or populations. It is a record in digital format that is theoretically capable of being shared across different health care settings. In some cases this sharing can be afforded by network-connect enterprise-wide information systems and other information networks or exchanges. EHRs may include a range of data, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal statistics like age and weight, and billing information [4].

Barriers and Challenges of e-Health Cloud

- According to case studies from different countries, there are many challenges and issues that need to be addressed for a successful implementation of e-Health Cloud. Security and privacy of information are other serious technical challenges. Challenges are identified as follows [18]:
- IT Infrastructural weakness plus Lack of qualified personnel and training courses.
- Lack of knowledge about the e-Health program.
- Lack of security and privacy of information plus Lack of strategic plans.
- Lack of policy and regulation for e-usage and Lack of partnership and collaboration.
- Resistance to change to e-Health Cloud Systems as well as the shortage of financial resources.

Stages of e-Health Cloud

In order to accomplish e-Health Cloud initiatives, there must be a phased approach applied to the infrastructure Development which transforms an initial e-Health Cloud initiative into final desired service. The following are the four stages of e-Health Cloud, which in most cases follow each other [19].

- Present the work on the Web: The first stage on any e-Health Cloud is marked by its presence on the web which acts as a common place for distributing information to the

public. It is the most basic part of any e-Health Cloud system and has limited capabilities.

- Interact with Citizen and Governments: The second stage is marked by the presence of an interactive web interface where some kinds of communication occur between government and its citizens through the web.
- Complete Transaction over Web: The stage involves transaction between a citizen and government being completed over the internet.
- Integrate Services: This is the highest level of any e-Health Cloud where technology is utilized to its full potential [20].

E-Health System in Cloud Computing

First of all we will discuss the components of the e-Health system in cloud computing that can be attacked such as the e-Health Cloud system, the communication channel and the patient's client (see Figure 1).

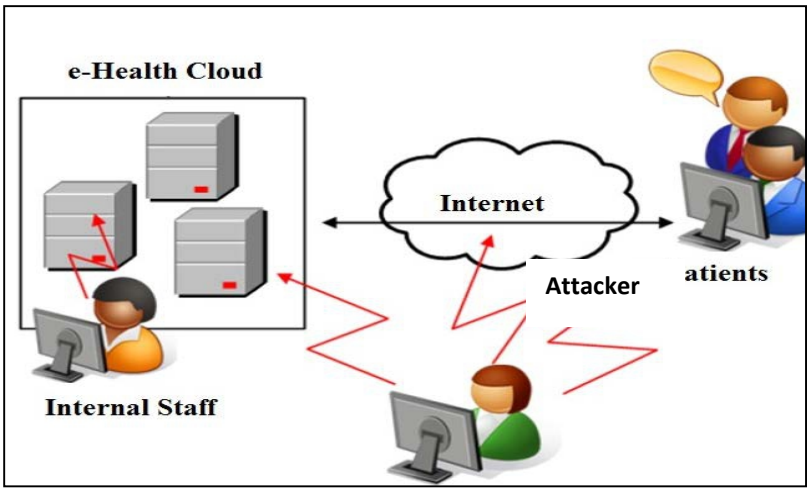

Figure 1: Attackers in Context of e-Health Cloud System

We distinguish between three different kinds of attackers:

Internal attackers: who have authorized access to network resources [8], e.g. operators of the system or medical staff, conduct attacks mainly against the e-Health system; these attacks are solely prevented by means of organizational measures when designing security concepts of e-Health systems in cloud computing.

External adversaries: they are usually considered when discussing security in context of e-Health systems. These adversaries can either behave actively, e.g. hackers, or passively, e.g. eavesdroppers. In contrast, to passive adversaries, who are only wiretapping the communication channel, active adversaries also manipulate transferred and stored data. It must be pointed out that, in general, it is easier for an insider to get unauthorized access to medical data than for an external adversary. Consequently, in order to establish a reliable security concept for an e-Health system in cloud computing, insider attacks need to be taken into consideration as carefully as external attacks.

Curious Person: this is introduced as a third kind of adversaries which has not been considered in architectures for e-Health system in cloud computing until now. These attackers will be denoted as "curious persons" in this paper.

A person who is trying to attack the e-Health system in cloud computing is an "attacker" who tries to obtain medical information about a person by influencing this person to present the medical data on their own. The relevance of attacks conducted by curious persons cannot be evaluated seriously. However, in our opinion this attack needs to be taken into consideration, since it cannot be excluded. This attack can be achieved by means of more

or less sophisticated methods. The former methods mainly comprise methods from social engineering, e.g. a curious person may convince a patient to hand out his login credentials to him. These attacks can only be prevented by raising awareness during security trainings. It must be noted that technical measures cannot be used to counter these attacks, since the attacked person does not perceive the situation as an attack.

Having identified security threats in e-Health system based on the security analysis in cloud computing, it is possible to define security properties which counter these threats. Thereby, we distinguish between basic and enhanced security properties. The basic security properties are those which are well known from standard security books on information systems and computer security. These comprise authentication and authorization, availability, confidentiality and integrity of data and are absolutely necessary in context of e-Health systems. However, it must be emphasized that these properties mainly protected against external adversaries but marginally against internal ones and not at all against curious persons. Therefore, it is inevitable to define enhanced properties to increase the level of security regarding the latter two groups of adversaries.

Enhanced Security Properties of e-Health Cloud

These comprise anonymity, deniability and unlink ability. We will briefly discuss these properties.

1. Anonymity: Frequently referred to as "buffer overruns," .This type of attack seeks to connect anonymously to a service and then elevate the attacker's privileges on the system to that of a valid user or an administrator. This type of attack exploits a weakness in the server code allowing attackers to execute arbitrary code that they've sent to the service. The code elevates their privileges and allows them to gain direct access [21]. Anonymity is often referred to as the property of being not identified with respect to a set of actions inside a group of people, the so called anonymity set. Intuitively the degree of anonymity is the higher, the larger the anonymity set is and the more uniformly the actions are distributed within this set.
2. Considering an e-Health Cloud system we can define anonymity at three different levels.
3. Anonymous communication: This type is guaranteed, if an observer is not able to determine a communication relationship between two communicating parties by means of information revealed by the communication channel.
4. Sender-receiver anonymity: A communication relationship between a sender and receiver provides sender-anonymity, if the receiver is not able to identify the sender by means of received messages.
5. Data anonymity: A system provides data anonymity, if data stored in the system of the receiver and related to a specific sender cannot be linked to the sender by the receiver and any other person.
6. Deniability: In context of medical data the term deniability means that an adversary is not able to prove the existence of medical data related to a specific person. This means that a patient can plausibly deny the existence of any medical data of his PHR and even internal adversaries are not able to figure out the existence of patient’s data. For instance, a patient can hide highly compromising information from a curious person who conducts a disclosure attack [22].
7. Unlinkability: Unlinkability of items of interest means that relations between items, where a priori exist, cannot be identified through pure observation of the system. A system containing n users provides perfect unlink ability, if the relation of an object and a user exists with probability p =1/n for all objects. Hence, an insider of the system cannot gain any information on links between users and objects by means of solely observing the system [22].

Privacy Domains for E-Health

In the context of e-Health, privacy protection of the patients' data is a primary concern. Technological solutions should be employed to support legal and contractual regulations. We propose to construct privacy domains for the patients' medical data as a technical measure to support the enforcement of privacy and data protection policies: Systems (e.g., a client PC) must be able to partition execution environments for applications into separate domains that are isolated from each other. Data is kept within a privacy domain, and the domain infrastructure ensures that only authorized entities can join this domain. Moreover, data leakage from the domain is prevented by the security architecture and the domain infrastructure. Therefore, the same system can be used for different work flows that are strictly isolated. Figure 2, illustrates the privacy domains applied to our e-Health Cloud model.

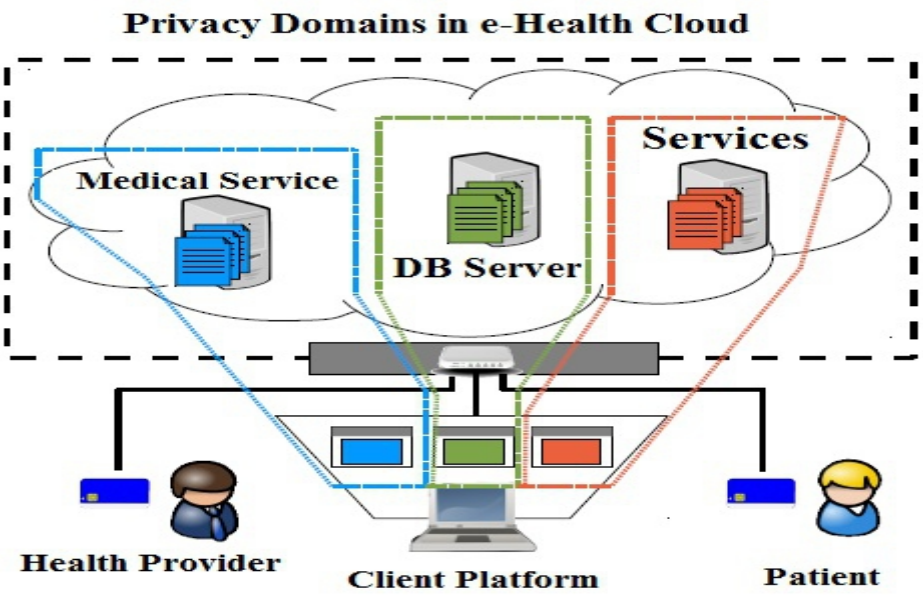

Figure 2: Privacy Domains in the E-Health Cloud

Conclusion

The traditional healthcare model is changing significantly driven by an aging population, funding constraints, greater demand for care and a greater awareness of medical errors. The industry will increasingly turn to ICT to meet these challenges. By using the cloud computing technology in a healthcare the industry may considerably improve the access to information, which can be done faster and easier. The scalability, that is the key of the cloud computing, can offer more resources needed for certain operation at any time. The collaboration between healthcare units is an opportunity offered by cloud computing for healthcare staff. This technology can be used to check the availability of a physician, a medical specialist, a product or a service at different times and in different cases. In this paper, we have provided a security analysis of e-Health systems in cloud computing. We have introduced enhanced security properties for e-Health systems.They could enable the e-Health care services provider to reduce maintenance cost by moving data to cloud storage which provides anytime, anywhere access to patient information. We discussed methods to realize them. In our opinion these enhanced properties are of enormous relevance when realizing a reliable e-Health Cloud system. Currently, we are investigating how to efficiently integrate the proposed methods into existing approaches and we are developing more efficient solutions for anonymous authentication and unlinkability.

References:

Hans, L., Sadeghi, A., & Winandy, M. Securing the E-Health Cloud. 1st ACM International Health Informatics Symposium. 2010.

Camous, F., Duignan, F., & Henry, P. An Ehrcom-Compliant Assessment tool for Community Nursing in Ireland. IADIS International Conference e-Health, 2009.

Barua, M., Liang, X. Enabling Security and Patient-centric Access Control for eHealth in cloud computing. Int. J. Security and Networks, Vol.1 IEEE INFOCOM'11-SCNC, 2011.

Gunter, D., & Terry, Nicolas P. The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. Journal of Medical Internet Research 7 (1), 2005.

Fingberg, J. & Hansen, M. Integrating Data Custodians in eHealth Grids – Security and

Habib, J. L. EHRs, meaningful use, and a model EMR. Drug Benefit Trends 22 (4): 99–101,

ICT for Health, Information Communication Technology, Newsletter June 2012.

Al-Khanjari, Z., Alanee, A., Kraiem, N. & Jamoussi, Y. Proposing a Real Time Internal Intrusion Detection System towards a Secured Development of E-Government Web Site. European Scientific Journal Vol.3, 2013.

Marcio, K., Emilio, F., Merino, C. , & Gerhard, W. A clinical field research oriented relational database to study of human malaria, IADIS International Conference e-Health,

Zhang, R. & Liu, L. Security Models and Requirements for Healthcare

Kilic, O., Dogac, A. & Eichelberg, M. Providing Interoperability of eHealthCommunities Through Peer-to-Peer Networks, IEEE TITB, 14(3), pp. 846–853,2010.

Goce, G. & Vladimir, T. Security and Privacy Issues and Requirements for Healthcare Cloud Computing, ICT Innovations 2012 Web Proceedings ISSN 1857-7288, 2013.

Ravij, K., Nishant, S. & Sutaria, K. Ameliorate Security Policy Using Mediated RSA and Identity Based Cryptography in Cloud Computing , Journal of information, knowledge and research in computer engineering, 2, ISSN: 0975 – 6760, pp. 389, October, 2013.

Singh, H. & Bansal, B. Analysis of security issues and performance enhancement in cloud Computing, International Journal of Information Technology and Knowledge Management,

Malpani, G. Cloud Computing: Key to Business Fitness, Paripex - Indian

Journal of Research, 3(4), ISSN - 2250-1991, May, 2013.

Khaja, S., Khamruddin, M. & Krishna, K. An Overview of Data Security in Cloud Computing, International Journal of Advances in Computer, Electrical and Electronics Engineering, 2, ISSN: 2248-9584, December, 2012.

Steve, G. Cloud Computing, Oxford University, England, International journal of Innovative Research in Engineering and Science, 1(1), ISSN 2319-5665,

Nugi Nkwe, E-Government: Challenges and Opportunities in Botswana Department of Accounting and Finance University of Botswana Gaborone, Botswana International Journal of Humanities and Social Science 2(17); September 2012.

Beji, S., Jamoussi, Y. & El Kadhi, N. : Towards context-awareness security for mobile applications, The International Conference on Service, Security and its Data management technologies in Ubi-com, IEEE, China, October 2010.

Sami M. Alhomod and Mohd Mudasir Shafi: Best Practices in E government: A review of Some Innovative Models Proposed in Different Countries International Journal of Electrical

Al-Ani, A. Real Time Internal Intrusion Detection in Web Site, Congress of Scientific Research Outlook in the Arab World "Scientific Innovation and Sustained Development,

Slamanig, D. & Stingl, S., Sophisticated Methods To Prevent Insider Attacks Against Phr Systems, Iadis International Conference e-Health, 2009.